United Nations S/2004/296

Security Council

Distr.: General
15 April 2004

Original: English

Letter dated 14 April 2004 from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

I write with reference to my letter of 14 January 2004 (S/2004/36). The Counter-Terrorism Committee has received the attached third report from the United States of America submitted pursuant to paragraph 6 of resolution 1373 (2001) (see annex).

I would be grateful if you could arrange for the present letter and its annex to be circulated as a document of the Security Council.

(*Signed*) Inocencio F. **Arias**
Chairman
Security Council Committee established pursuant to
resolution 1373 (2001) concerning counter-terrorism

04-31335 (E) 270504

Annex

Letter dated 1 April 2004 from the Chargé d'affaires a.i. of the United States Mission to the United Nations addressed to the Chairman of the Counter-Terrorism Committee

Enclosed is the third report of the United States to the Counter-Terrorism Committee (see enclosure). The report is in response to the Committee's letter dated 29 December 2003. The United States looks forward to continued cooperation with the Committee.

(*Signed*) James B. **Cunningham**
Chargé d'affaires a.i.

Enclosure

Reply to the Counter-Terrorism Committee, 1 April 2004

Security Council Resolution 1373 (2001)

Implementation measures

1.1 Ratification of international conventions: Sub-paragraph 3 d) of the Resolution calls upon States to become parties as soon as possible to the relevant international conventions and protocols relating to terrorism. In that regard, the CTC would be grateful for a further progress report on the enactment and implementation in US law of the two international instruments mentioned in the second report and recently ratified:

- *The UN Convention for the Suppression of Terrorist Financing;*
- *The UN Convention for the suppression of Terrorist Bombings;*

On June 25, 2002, President Bush signed into law legislation (Public Law 107-197) that implemented two United Nations conventions relating to terrorism. Title I of Public Law 107- 197, the "Terrorist Bombings Convention Implementation Act of 2002," created a new Section 2332f in Title 18, United States Code (Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities). Title II of Public Law 107-197, the "Suppression of the Financing of Terrorism Convention Implementation Act of 2002," created a new Section 2339C in Title 18, United States Code (Prohibitions against the financing of terrorism). The United States deposited its instruments of ratification for both of these conventions on June 25, 2002, and both conventions entered into force for the United States on July 26, 2002. Both statutes supplement existing federal and state law and do not supplant any other law.

Effectiveness in the protection of the financial system

1.2 In the context of the implementation of Sub-paragraph 1 d) which prohibits the making of funds available to terrorists, the CTC is aware that the United States may have recently been evaluated by organizations involved in the protection of financial systems against abuse by criminals and, in particular, against abuse by people or entities intent on directing funds towards the financing of terrorism.

The CTC would appreciate receiving a copy of any evaluation or reports produced by these organizations.

No recent outside evaluations of the U.S. anti-money laundering and counter-terrorist financing (AML/CFT) system have been conducted.

1.3 In this regard, what measures have been taken by the United States to implement the recommendations expressed by the FATF after the second mutual evaluation during FATF-VIII (1996-1997)?

It is important to note that the second FATF mutual evaluation was based on a set of Recommendations that have been subsequently updated. In June 2003, the FATF endorsed a revised set of Forty Recommendations Against Money Laundering. In addition, FATF developed the Eight Special Recommendations Against Terrorist Financing in October 2001, elements of which overlap with UNSCR 1373 and have been addressed in previous submissions to the CTC.

That said, the United States has made significant progress in addressing weaknesses identified in the 1996-1997 Mutual Evaluation. In fact, in many areas, measures taken to date exceed compliance with the standards contained in the Revised 40 Recommendations. In response to this question, areas of concern that will be addressed include the sufficiency of AML requirements for particular non-bank financial institutions, suspicious transaction reporting and "know your customer" rules.

The 2001 USA PATRIOT Act (Public Law 107-56 – the "Act") contains a mandate for Treasury to expand its AML regime to all financial institutions as defined by the Bank Secrecy Act (BSA). The BSA defines financial institutions broadly to include such businesses as depository institutions; securities brokers; futures brokers; mutual funds; insurance companies; investment companies; travel agents; dealers in precious stones, metals and jewels; and vehicle sellers. In particular, section 352 of the Act requires all financial institutions to have an AML program. Under the statute, the AML program must include: (1) the development of internal policies and procedures; (2) the designation of a compliance officer; (3) an employee training program; and (4) an independent testing function to verify that the program is operating as required.

Insurance Sector

The U.S. Treasury Department issued a proposed regulation on September 26, 2002, to extend AML controls to certain insurance companies (namely, companies that deal in life insurance and annuities). (See, "Anti-Money Laundering Requirements for Insurance Companies," http://www.fincen.gov/352 insurance.pdf). The proposed rule will require certain insurance companies to assess the money laundering and terrorist financing risks posed by its products, distribution channels, and customer base. The proposed rule also requires insurance companies to incorporate policies, procedures, and internal controls integrating its agents and brokers into its AML program. The rule sets forth the minimum requirements of an insurance company's AML program. For example, it requires that an insurance company designate a compliance officer to be responsible for the administration of the AML program, and provides for education and training of appropriate persons. In addition, the rule requires that an insurance company provide for independent testing of its program on a periodic basis to ensure that it complies with the requirements of the rule and that the program functions as designated.

On October 17, 2002, the U.S. Treasury Department issued a proposed rule that would require insurance companies to file suspicious activity reports and stipulates that insurance companies shall maintain a copy of any suspicious transaction report filed, and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing. (See, "Requirement that Insurance Companies Report Suspicious Transactions," http://www.fincen.gov/insurance_sar.pdf) The proposed rule mirrors existing suspicious activity reporting rules for other financial institutions, and is designed to encourage the reporting of transactions that appear relevant to violations of law or regulation. Thus, if a transaction is unusual, complex or lacking any apparently legal purpose, the transaction should be reported. Records would be kept for a variety of transactions, beyond simply "large transactions." In addition, the proposed rule discussed above requiring an anti-money laundering program would require all affected insurance companies to focus on transactions that are worthy of further scrutiny and keep. An insurance company would be required to make all supporting documentation available to the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), any other appropriate law enforcement agencies, or state regulators upon request.

Bureaux de Change and Money Transmitters

The U.S. Treasury Department issued on March 14, 2000, a final rule requiring that all money transmitters to file suspicious activity reports relevant to violations of law or regulations, and encourages this even in cases falling below the threshold in the rule. (See, "Requirement that Money Transmitters and Money Order and Traveller's Check Issuers, Sellers, and Redeemers Report Suspicious Transactions," http://www.fincen.gov/msbreg.pdf). An identical rule for bureaux de change was also issued in final form on February 10, 2003. ("Requirement that Currency Dealers and Exchangers Report Suspicious Transactions," http://www.fincen.gov/sar_currency_exch021003.pdf). Bureaux de change must be in full compliance with the rule by August 13, 2003.

The United States has issued extensive guidelines to money service businesses (MSBs), including bureaux de change and money remitters. This guidance includes the following:

- "Bank Secrecy Act Requirements – A Quick Reference Guide for MSBs" (http://www.fincen.gov/bsa_quickrefguide.pdf)
- "Reporting Suspicious Activity – A Quick Reference Guide for MSBs" (http://www.fincen.gov/msbsar_quickrefguide.pdf)
- "Money Laundering Prevention – An MSB Guide" (http://www.fincen.gov/msb_prevention_guide.pdf)

Stockbrokers

The U.S. Treasury Department issued a final rule on July 1, 2002, requiring securities brokers to file suspicious transaction reports with the U.S. government. (See, "Requirement that Brokers or Dealers in Securities Report Suspicious Transactions," http://www.fincen.gov/brokerdealersarjuly2002.pdf).

Mechanisms for strengthening the SAR system

The United States issues general suspicious activity reporting guidance to all financial institutions, including money service businesses. These include the following:

- *Suspicious Activity Reporting Guidance for Casinos:* http://www.fincen.gov/casinosarguidancefinal1203.pdf
- *Guidance on Preparing Suspicious Activity Reports:* http://www.fincen.gov/narrativeguidance_webintro.pdf
- *The SAR Activity Review – Trends, Tips and Issues:* http://www.fincen.gov/sarreviewissue6.pdf. This guidance is published twice a year.
- *Reporting Suspicious Activity – A Quick Reference Guide for MSBs* http://www.fincen.gov/msbsar_quickrefguide.pdf

Measures to Guard Against Criminals Gaining Control of Insurance Companies, Bureaux de Change and Money Transmitters:

It is a crime in the United States for the officers of an insurance company to be convicted felons, unless the government has explicitly granted a waiver in a particular case. Additionally, money service businesses are required to be registered with FinCEN (See, 31 U.S.C. 5330, http://www4.law.cornell. edu/uscode/31/5330.html and http://www.fincen.gov/msbreg1.pdf) and as of April 29, 2002 to have anti-money laundering compliance programs. (See, "Anti-Money Laundering Compliance Programs for Money Services Businesses," http://www.fincen.gov/352msb.pdf). FinCEN has also been engaged in a multi-year education program to disseminate information to MSBs regarding registration and SAR requirements. FinCEN places a high priority on effective and broad-reaching initiatives to facilitate the education of MSBs and their agents in their responsibilities under the Bank Secrecy Act. Therefore in July 2003 FinCEN proposed a survey intended to evaluate the success of the MSB education program (http://www.fincen.gov/ msbfinsurveyfedreg072203.pdf). The U.S. Government regards these measures as adequate to address the associated risks. An MSB Registration List has also now been published including all entities that have registered as MSBs, from December 2001 through January 9, 2004, pursuant to FinCEN's Bank Secrecy Act (BSA) rules at 31 CFR 103.41 (http://www.msb.gov/pdf/ msbregistration_introletter.pdf).

Customer Identification Requirements

In May 2003, the U.S. Treasury Department published several Final Rules requiring new customer identification programs for a variety of types of financial institutions and

non-bank financial institutions, several of which go beyond the Revised 40 Recommendations:

- *Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks* (Joint Final Rule) - May 9, 2003 (http://www.fincen.gov/326bankfinal.pdf)
- *Customer Identification Programs for Broker-Dealers* (Joint Final Rule) - May 9, 2003 (http://www.fincen.gov/326bdfinal.pdf)
- *Customer Identification Programs for Mutual Funds* (Joint Final Rule) - May 9, 2003 (http://www.fincen.gov/326mffinal.pdf)
- *Customer Identification Programs for Futures Commission Merchants and Introducing Brokers* (Joint Final Rule) - May 9, 2003 (http://www.fincen.gov/326fcmfinal.pdf)
- *Customer Identification Programs for Certain Banks Lacking a Federal Functional Regulator* (Notice of Proposed Rulemaking) - May 9, 2003 (http://www.fincen.gov/326banknoffr.pdf)

Additional Measures Taken by The United States

- *Anti-Money Laundering Programs for Investment Advisers* (Proposed Rule) - May 5, 2003 (http://www.fincen.gov/352investmentadvisers_fedreg050503.pdf)
- *Anti-Money Laundering Programs for Commodity Trading Advisors* (Notice of Proposed Rulemaking) - May 5, 2003 (http://www.fincen.gov/352commoditytrading_fedreg050503.pdf)
- *Requirement that Futures Commission Merchants and Introducing Brokers in Commodities Report Suspicious Transactions* (Notice of Proposed Rulemaking) - May 5, 2003 (http://www.fincen.gov/ futcombrokers_sar_fedreg050503.pdf)
- *Anti-Money Laundering Program Requirements for "Persons Involved in Real Estate Closings and Settlements"* (Advance Notice of Proposed Rule) - April 10, 2003 (http://www.fincen.gov/352_real_estate_04102003.pdf)
- *Anti-Money Laundering Programs for Travel Agencies* (Advance Notice of Proposed Rule) - February 24, 2003 (http://www.fincen.gov/pa_352_travel_agencies.pdf)
- *Anti-Money Laundering Programs for Businesses Engaged in Vehicle Sales* (Advance Notice of Proposed Rule) - February 24, 2003 (http://www.fincen.gov/pa_352_vehicle_sales.pdf)

- *Anti-Money Laundering Programs for Dealers in Precious Metals, Stones or Jewels* (Notice of Proposed Rule) - February 21, 2003 (http://www.fincen.gov/pa_352_jewelry.pdf)
- *Anti-Money Laundering Requirements -- Correspondent Accounts for Foreign Shell Banks; Recordkeeping and Termination of Correspondent Accounts for Foreign Banks* (Final Rule) - September 26, 2002 (http://www.fincen.gov/sec313-319finalrule.pdf)
- *Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity* (Final Rule) - September 26, 2002 (http://www.fincen.gov/section314finalrule.pdf)
- *Anti-Money Laundering Programs for Unregistered Investment Companies* (Notice of Proposed Rule) - September 26, 2002 (http://www.fincen.gov/ 352insurance.pdf)
- *Special Due Diligence Programs for Certain Foreign Accounts* (Interim Final Rule) - July 23, 2002 (http://www.fincen.gov/section312interim.pdf)
- *Anti-Money Laundering Programs for Mutual Funds* (Interim Final Rule) - April 29, 2002 (http://www.fincen.gov/352mufunds.pdf)
- *Anti-Money Laundering Programs for Operators of a Credit Card System* (Interim Final Rule) - April 29, 2002 (http://www.fincen.gov/ 352ccards.pdf)
- *Amendment to Bank Secrecy Act Regulations -- Requirement that Nonfinancial Trades or Businesses Report Certain Currency Transactions* (Interim Rule, Final and Proposed Rules) - December 31, 2001 (http://www.fincen.gov/fedreg123101nonfintrades2.pdf)
- *Requirement That Mutual Funds Report Suspicious Transactions* (Notice of Proposed Rulemaking and Request for Comments) - January 21, 2003 (http://www.fincen.gov/mufund_sar_nprm.pdf)
- *Requirement that Casinos & Card Clubs Report Suspicious Transactions* (Final Rule) - September 26, 2002 (http://www.fincen.gov/casinosarfinal rule.pdf)

Effectiveness of counter-terrorism machinery

1.4 Anti-terrorist strategy: Sub-paragraph 2 b) of the resolution requires States to take steps to prevent the commission of terrorist acts. In this regard, please outline any special anti-terrorist policies which the United States has developed aimed at preventing the commission of terrorist acts in the following areas:

- *Links between terrorism and other criminal activities;*

- *Physical protection of potential terrorist targets;*
- *Strategic analysis and forecasting of emerging threats;*

In October of 2001, the United States passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the USA PATRIOT Act), which seeks to provide tools to assist law enforcement and other agencies in combating terrorism. The USA PATRIOT Act does this in three primary ways: First, it closes gaps in the United States Government's ability to investigate terrorists. Second, the USA PATRIOT Act updates United States anti-terrorism laws to meet the challenges presented by new technologies and new threats. Third, the USA PATRIOT Act allows for expanded information sharing among government agencies for purposes of terrorism-related investigations.

- *Criminal investigation and prosecution;*

The USA PATRIOT Act enhances the ability of investigators to fight terror. For instance, the Act allows federal agents to conduct anti-terrorism investigations without immediately notifying the subject of a search that the search has been conducted. If criminals learn too early of an investigation, they might flee, destroy evidence, intimidate or kill witnesses, cut off contact with associates, or take other action to evade detection or arrest. Federal courts in narrow circumstances have long allowed law enforcement agencies to delay, for a limited time, informing the subject that a court-approved search warrant has been executed. Although delayed notification search warrants have been upheld by courts as fully consistent with the protections of the Constitution, not all courts have been willing to issue them. This lack of uniform acceptance is corrected by the USA PATRIOT Act. Of course, notice of searches is ultimately provided, but the reasonable delay gives law enforcement agencies time to identify the suspect's associates, eliminate immediate threats to our communities, and coordinate the arrests of multiple individuals without tipping them off prematurely.

Another tool the USA PATRIOT Act provides is court-approved access to business records to protect against international terrorism or clandestine intelligence activities. For example, investigators may need to look at records from chemical plants or hardware stores to discover who bought materials that could be used to construct a bomb, or law enforcement may need bank records to follow the trail of money being sent to terrorist organizers abroad. For many years, prosecutors have been able to obtain the business records in criminal cases by using grand jury subpoenas. However,

before the USA PATRIOT Act, agents had limited tools to obtain such records in national security terrorism investigations. The USA PATRIOT Act recognized that the same type of records should be available in national security investigations as well as in criminal investigations, while providing special consideration for activities protected by the First Amendment.

- *Links between Terrorism and other criminal activities*

The USA PATRIOT Act aimed to address terrorism through the investigation and prosecution of other criminal activities that are linked to or facilitate terrorist acts. One of the most notable crimes linked to terrorism is money laundering, since revenues from illegal acts have been used to finance terrorism in the past. Title III of the USA PATRIOT Act, which is also know as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, provides the U.S. Federal Bureau of Investigation (FBI) with the necessary tools to fully investigate money laundering cases that have a terrorism nexus.

In addition, the FBI has been restructured to better address terrorist financing matters. During the early stages of the 9/11 investigation, the FBI and the Department of Justice (DOJ) identified a critical need for a more comprehensive, centralized approach to terrorist financial matters. In response, the FBI established an inter-agency Terrorism Financial Review Group (TFRG), operating out of FBI Headquarters. The TFRG brought together vast financial, intelligence and other databases and made them available to the investigatory experts in numerous federal agencies. The TFRG was expanded and then renamed the Terrorist Financing Operations Section (TFOS). It is part of the FBI's Counterterrorism Division, and focuses a powerful array of resources on the financial dealings and interests of terrorist organizations.

- *Physical Protection of Potential Terrorist Targets*

While the United States and our allies continue to direct actions against terrorists and their infrastructures abroad, we are simultaneously strengthening the security of the homeland.

Since September 11, 2001, the President has signed numerous critical pieces of legislation into law to improve homeland security, most notably the Homeland Security Act of 2002 (Public Law 107-296). The Act established a cabinet-level Department of

Homeland Security dedicated to preventing, mitigating, and responding to terrorist attacks on the United States.

The President also has developed a robust policy framework to address terrorism in the United States. The cornerstone of this policy framework is *The National Strategy for Homeland Security*, which served to mobilize and organize the efforts of federal, state, local, and private organizations around the national goal of protecting the homeland, including the protection of critical infrastructure and key assets. The major critical infrastructure protection initiatives called for by the *Strategy* were the unification of protection efforts within the Department of Homeland Security, building and maintaining assessments of all critical infrastructure and key assets, developing effective partnerships at all levels of government and the private sector, developing a national plan for infrastructure protection, harnessing the best analytic and modeling tools for protective efforts, guarding critical infrastructure and key assets against "inside" threats, and partnering with the international community.

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets refined the national approach to protecting critical infrastructure and key assets from physical attack. The policy adheres to the following strategic objectives: 1) identify and assure the protection of those infrastructures and assets that are most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence consequences; 2) provide timely warnings and assure the protection of infrastructures and assets that face a specific threat; and 3) foster a collaborative environment in which all levels of government and the private sector can effectively protect the infrastructure and assets they control, according to their specific responsibilities, competencies, and capabilities. The strategy complements *The National Strategy to Secure Cyberspace*, which focuses on the identification, assessment, and protection, of interconnected information systems and networks.

Finally, *Homeland Security Presidential Directive (HSPD) 7* established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attacks. Protective actions include a wide range of activities designed to reduce the vulnerability of critical infrastructures in order to deter, mitigate, or neutralize terrorist attacks. *HSPD-7* assigns to the Department of Homeland Security the responsibility for leading, integrating, and coordinating the implementation of protective efforts among federal

departments and agencies, state and local governments, and the private sector. It also tasks federal departments and agencies with protection activities in designated critical infrastructure sectors. All of these efforts will be accomplished in cooperation with state and local governments and the private sector. *HSPD-7* includes an emphasis on the protection of terrorist targets, attacks on which might result in catastrophic health effects and mass casualties.

- *Strategic Analysis and Forecasting of Emerging Threats*

Intelligence Analysts assigned to the Department of Homeland Security Office of Information Analysis (IA) within the Information Analysis and Infrastructure Protection (IAIP) Directorate monitor all source intelligence reporting on a daily basis. IA analysts monitor three different aspects of threat reporting. Terrorist network analysts research terrorist plans, threat streams, organizations, activities, member cells, and forms of support. Terrorist capabilities analysts monitor terrorist capabilities and develop hypotheses and research on potential capabilities. They produce assessments on attempts to develop or acquire nuclear, radiological, chemical, and biological materials for use in attacks. Critical infrastructure analysts assess the viability of terrorist threats, plans and intentions against key sectors and assets, and monitor terrorist plans and activities against infrastructure worldwide.

As a member of the U.S. Intelligence Community (IC) and in conjunction with other members of the IC, DHS/IA analysts monitor a series of strategic "threat themes" that address prominent threats to the homeland. Each of these themes is routinely monitored and updated in three areas: threat, vulnerabilities to threat, and actions taken to address the vulnerabilities. The threat is characterized by the known tactics the terrorists have used, the assessed capabilities of the terrorist to carry out the attack, the reported targets, and information gaps in intelligence reporting. The risk associated with each threat theme is assessed based on the intent and capabilities of the terrorist, the vulnerabilities of the target(s), and the consequences of an attack.

When a specific threat or threat stream is identified through the daily monitoring process, an assessment of the threat is evaluated from several different perspectives. The credibility of the reporting source is assessed. The intent and capabilities of the terrorist to carry out the reported threat are analyzed. In the case of nuclear radiological threats, the assessment includes the operational practicality of carrying out the attack, the technical feasibility of the attack, and the behavioral resolve of the terrorist(s).

Based on the assessment, additional actions may be taken to develop an advisory or information bulletin to distribute to other federal, and state, and local agencies, and private industry.

1.5 Has the United States encountered any difficulties as regards law enforcement and/or the gathering of intelligence in relation to the areas mentioned above? If so, please provide a brief description of what the difficulties were. The CTC would also find it helpful to receive information on recent successful operations in the areas above. In supplying such examples, States are not expected to supply information in respect of ongoing investigations or judicial processes if to do so would prejudice the proper conduct of an investigation or judicial process.

United States intelligence and law enforcement communities, and our partners, both here and abroad, have identified and disrupted over 150 terrorist threats and cells. Worldwide, more than 3,000 terrorist operatives have been incapacitated.

Four terrorist cells in Buffalo, Detroit, Seattle, and Portland (Oregon), have been broken up; 300 individuals have been criminally charged in the United States in terrorism investigations; 163 individuals have been convicted or have pled guilty in the United States, including shoe-bomber Richard Reid and "American Taliban" John Walker Lindh.

1.6 Improved coordination at home: The CTC is encouraged to note that the United States is engaged in an effort to improve its ability to combat terrorism and has set up since 2001 a reorganization plan of its departments and agencies dealing with this issue. The CTC would be grateful to receive an outline of the results of this new organization. In particular, has the United States created appropriate mechanisms to ensure adequate co-operation and information sharing among the different government agencies which may be involved in investigating the Financing of Terrorism?

A detailed reorganization plan (pursuant to section 1502 of the Department of Homeland Security Act of 2002) was unveiled on November 25, 2002. The complete plan can be found on the worldwide web at: http://www.whitehouse.gov/news/releases/2002/11/reorganization_plan.pdf. Also, see the information on the creation of TFOS within the FBI as described under section 1.4, above.

Although based on broader considerations than terrorist financing, the provisions of the USA PATRIOT Act which address improved sharing of information between law enforcement and intelligence components and agencies serve to facilitate the improved integration of information relating to all aspects of terrorist activity.

Additionally, in early 2003, a Terrorist Threat Integration Center (TTIC) was created pursuant to the direction of the President. TTIC institutionalizes the sharing of threat-related information across federal agency lines, thereby enabling full integration of terrorist threat information and analysis.

Finally, the Attorney General's Global Justice Information Sharing Initiative Advisory Committee, in collaboration with law enforcement executives and intelligence experts at the federal, state, and local levels, developed the National Criminal Intelligence Sharing Plan to facilitate information sharing among different government agencies. The Plan outlines model policies, standards, and guidelines for developing a law enforcement intelligence function at the local level, includes in-depth discussions and recommendations on key implementation issues and barriers, and emphasizes better methods for developing and sharing critical data. The Plan will improve the ability of the United States to respond to criminal activity and terrorism, including the financing of terrorism. Further information may be obtained at http://it.ojp.gov/index.jsp.

1.7 Criminal proceedings: Sub-paragraph 2 e) requires States to ensure that terrorists and their supporters are brought to justice. Are there any special counterterrorist measures applicable in criminal proceedings? Does the United States train its administrative, investigative, prosecutorial and judicial authorities to enforce its laws in relation to:

- *Typologies and trends in terrorist financing methods and techniques?*
- *Techniques for tracing criminal properties and funds with a view to seizing and confiscating them?*

Special counterterrorist measures:

The U.S. Marshals Service (USMS) is responsible for the security of U.S. federal court proceedings. Since 9/11, the USMS has provided security for several terrorist-related proceedings. The USMS relies on three internal units to provide extra security, to counter surveillance, and to detect and respond to a chemical, biological, radiological, nuclear or high-yield explosive situation within a courthouse. The USMS increased its

ability to respond to incidents involving chemical, biological, radiological, nuclear or high-yield explosives in courthouses by expanding its Hazardous Response Unit (HRU) from 2 to 14. HRU is a group of highly trained, self-sustainable deputies capable of responding anywhere in the U.S. or its territories. All HRU members are certified to operate in hazardous environments and each member is certified as an Emergency Medical Technician or paramedic. HRU possesses highly technical equipment capable of collecting, testing and mitigating chemical and biological agents. It is capable of providing environmental screening, monitoring, rescue and decontamination during these trials. HRU members are certified to conduct WMD vulnerability assessments for courthouses holding terrorist or terrorist-related proceedings.

The Special Operations Group (SOG) is a team of highly trained and mobile tactical response personnel. One of its missions is to provide tactical support to judicial districts holding terrorist or terrorist-related proceedings. It provides prisoner escort, personal protection for court personnel and witnesses, and assists with physical security of the courthouse.

The Technical Operations Group (TOG), as one of its missions, provides technical support and counter-surveillance equipment for courthouses housing terrorist or terrorist related proceedings.

Turning to pertinent efforts of the U.S. Bureau of Alcohol, Tobacco, and Firearms (ATF), one of its strategic goals is to reduce the rising trend in the illegal diversion of alcohol and tobacco products and thereby decrease the resulting profits that are used to further criminal and terrorist schemes. In connection with the President's Executive Order on Terrorist Financing, ATF has been investigating individuals and businesses involved in the trafficking of illicit cigarettes to determine any possible ties or associations with named terrorist groups or their supporters was occurring. Since the events of September 11, 2001, ATF has investigated suspects in 223 cigarette diversion cases to determine whether there is evidence of material support to terrorist organizations.

These schemes can generate tremendous cash profits. For example, a truckload of cigarettes will yield more than $1.2 million in profit if federal and state taxes have been avoided. U.S. and state cigarette tax losses are estimated by some at $1.4 billion. The terrorist aspect of revenue loss attributed to illicit tobacco trafficking cannot be estimated. Prior to the events of September 11, 2001, the World Bank estimated that

governments around the world would lose approximately $24 to $30 billion annually in uncollected tax revenue. Current indications disclose that terrorist groups are engaged in tobacco diversion and forming alliances with tobacco traffickers to generate monies used to support their organizations and activities.

Within the past 5 years, ATF has initiated approximately 500 tobacco trafficking investigations, seized more than $8.1 million in contraband cigarettes, and forwarded 286 defendants for prosecution. In one case, concluded in December 2003, Hassan Makki was sentenced to 57 months' imprisonment and fined over $600,000 and Elias Mohamad Akhdar of Dearborn, Michigan, was sentenced to 70 months in prison, both for providing material support to the designated foreign terrorist organization, Hizballah, and for conspiring to violate the Racketeering Influenced and Corrupt Organization Act (RICO) as a result on involvement in the smuggling of contraband cigarettes. In another case, concluded in March 2002, Haissam Nashar, of Charlotte, North Carolina, pled guilty in federal court to transporting counterfeit cigarette tax stamps and testified against Mohamad Hammoud in his use of illicit cigarette trafficking to support the terrorist group Hizballah. Approximately $1.5 million in assets was seized in this investigation.

ATF's presence in the contraband cigarette trafficking arena is fundamental to disrupting and eliminating criminal and terrorist organizations by identifying, investigating and arresting offenders who traffic in contraband cigarettes, and identifying for seizure and forfeiture assets used and proceeds of these crimes.

Training:

The Asset Forfeiture and Money Laundering Section (AFMLS) of the Criminal Division of the Department of Justice conducts approximately 24 seminars per year covering asset forfeiture, money laundering (including lectures on trends and techniques in money laundering and terrorist financing), and financial investigations. Participants in these seminars include prosecutors, law enforcement agents and support staff. AFMLS attorneys are recognized as domestic and international experts in the field of money laundering, asset forfeiture and terrorist financing. This area of the law is technical and constantly changing, and the advice and training AFMLS offers are in high demand. AFMLS provides invaluable assistance to federal prosecutors and law enforcement agents, as well as foreign law enforcement officials, in the areas of financial investigations, and money laundering and asset forfeiture laws. In addition to

the seminars sponsored by AFMLS, section attorneys routinely participate as speakers in other agencies and countries' conferences on terrorist financing, money laundering and asset forfeiture.

Examples of such training include:

Law Enforcement Training: In FY 2002 AFMLS conducted 12 seminars and trained over 1,185 federal prosecutors, federal agents, foreign officials, and state and local agents on forfeiture and money laundering law and financial investigations. In FY 2003, it conducted 11 seminars, reaching approximately 1,286 individuals.

Organized Crime Drug Enforcement Task Force (OCDETF) Training: AFMLS, in partnership with the Executive Office for OCDETF, is currently undertaking a major financial investigations training initiative and will conduct 24 financial investigations conferences around the country in 2004 and 2005, training approximately 2000 federal law enforcement agents and prosecutors.

International training and forfeiture sharing: AFMLS has developed significant international contacts by conducting annual regional international conferences to foster joint asset forfeiture and money laundering investigations. The most recent conference was conducted in South Africa in February 2004, and focused on money laundering and asset forfeiture related to political corruption cases. In the Fall of 2002, AFMLS held a conference in London which focused on terrorist financing and included representatives from European, Middle Eastern, and Asian countries. Previous conferences have been held in Hong Kong, Thailand, Costa Rica, and Argentina.

Development of Computer-Based Training: AFMLS is also developing computer-based training in asset forfeiture, money laundering and financial investigations for law enforcement agents and prosecutors.

Publications: In 2002, as part of a corroborative effort among the Counterterrorism Section, AFMLS and the United States Attorney's Office for the District of the Virgin Islands, a book entitled *Money Laundering and Terrorist Financing* was prepared for use by prosecutors and law enforcement. Additionally, AFMLS publishes the *Asset Forfeiture Quick Release* (monthly), the *Asset Forfeiture News* (bi-monthly), and the *Money Laundering Monitor* (semi-annually), as well as compendia of asset forfeiture and money laundering cases, which give the law enforcement community the best and

most timely information and advice in money laundering and asset forfeiture law and practice. The ever-growing demand for these resources makes clear that AFMLS will continue these endeavors.

Additionally, the Office of Justice Program's Bureau of Justice Assistance (BJA), Department of Justice, through the State and Local Anti-Terrorism Training (SLATT) Program, provides specialized training for law enforcement personnel in combating terrorism and extremist criminal activity. SLATT, a joint effort with the Federal Bureau of Investigation, focuses on the prevention of terrorism in the United States by providing the tools necessary for state and local law enforcement officers to understand, detect, deter, and investigate acts of terrorism in the United States by both international and domestic terrorists.

Training is offered in the following areas:

- Investigative/Intelligence Workshops. Designed for state and local law enforcement investigators, intelligence officers, and analytical personnel, this workshop includes topics related to the unique peculiarities inherent in the investigation and prosecution of terrorist and criminal extremist activity.

- Narcotics Task Force Anti-Terrorism Briefings. Designed for multi-jurisdictional narcotics task force personnel, this briefing combines terrorism awareness and investigative training with the expertise, experience, and contacts of narcotics task force groups to aid in the investigation, interdiction, and prevention of terrorist and extremist-related crimes.

- Train-the-Trainer Workshops. Designed for qualified law enforcement trainers, this workshop is intended to assist agencies in developing in-house anti-terrorism training capabilities and provides law enforcement trainers with the ability and information (i.e., lesson plans, sample notebooks, presentation materials, reference materials, etc.) to train other law enforcement personnel.

To date, 40,000 law enforcement personnel have been trained.

Effectiveness of customs, immigration and border controls

1.8 Sub-paragraph 2(g) requires States to have in place effective border controls in order to prevent the movement of terrorists and terrorist groups. In this regard:

(a) Would the United States please outline how it implements the common standards set by the World Customs Organization in relation to electronic reporting and the promotion of supply chain security?

The United States through Department of Homeland Security's U.S. Customs and Border Protection (CBP) is an active participant in World Customs Organization (WCO) activities related to Supply Chain Security. WCO Supply Chain Security consists of several WCO initiatives: Advance Cargo Information (ACI) Guidelines, the WCO Customs Data Model, and the WCO Unique Consignment Reference (UCR) Guidelines. CBP delegates to the WCO have ensured that United States requirements (24 hour rule) are congruent with the ACI guidelines. In addition, data requirements for CBP's Automated Commercial Environment (ACE) and the International Trade Data System (ITDS) will be included version 2.0 of the WCO Data Model in June 2005. At this time, CBP and traders will be able to use WCO data and EDIFACT messages for the receipt and transmission of the international harmonized data set.

CBP has been involved with automation of the cargo processing procedures since the early 1980's. Since then it has progressed to a state where over 99% of all cargo entries (goods declarations) are received electronically, over 90% of all inward vessel and rail manifests are electronic, and approximately 50% of air manifests as well. CBP has also negotiated arrangements with the largest air courier companies to make use of their internal computer systems to track and target many of the smaller shipments that are not currently tracked in CBP's Automated Commercial System.

CBP has incorporated the interchange of data on transportation and on goods within its systems to keep carriers well informed on the release status of importers' goods and has also allowed carriers to submit information on transit merchandise as well.

Under the 24-Hour Cargo Declaration Rule, CBP has not only begun to receive shipment data earlier in the transportation movement, but has also allowed more trade parties to automate with CBP and has increased the level of electronic communication among trade parties through CBP's systems.

New legislation and regulation will soon mandate the submission of all manifest information electronically. CBP is making the changes necessary to not only receive data from carriers and couriers electronically, but also improve the level of communication between the government and the trade parties involved in each transaction.

This increased level of automation of data will be combined with new accomplishments in electronic sealing and tracking of containers and vehicles. The data will be shared with other U.S. government agencies, such as the Coast Guard, to aid in the targeting and tracking of vessels and other conveyances as well. CBP utilizes a sophisticated "layered defense" strategy in protecting our borders against the threat of terrorism and in promoting global supply chain security.

On November 27, 2001, U.S. Customs Service Commissioner Robert C. Bonner introduced the Customs-Trade Partnership Against Terrorism (C-TPAT) program at the Customs Trade Symposium in Washington, D.C. Mr. Bonner challenged Customs and the trade community to design a new approach to supply chain security that would strengthen our borders while continuing to facilitate the legitimate flow of persons, cargo and conveyances. Since that time, the C-TPAT program has been implemented and over 5,500 members of the international trade community have become members.

Under the C-TPAT initiative, Customs is working with importers, carriers, brokers, and other industry sectors to develop a seamless security-conscious environment throughout the entire commercial process. By providing a forum in which the business community and Customs can exchange anti-terrorism ideas, concepts and information both the government and business community will increase the security of the entire commercial process from manufacturing through transportation and importation to ultimate distribution. This program underscores the importance of employing best business practices and enhanced security measures to eliminate the trade's vulnerability to terrorist actions.

C-TPAT is a cooperative endeavor. The program calls upon the trade community to establish procedures to enhance their existing security practices and those of their business partners involved in the supply chain. Once these procedures are in effect, imports of C-TPAT members may qualify for expedited Customs processing and reduced exams at ports of entry.

In addition, there are several other CBP layers that are deployed simultaneously to support supply chain security and substantially increase the likelihood that weapons of mass destruction (WMD) will be detected:

- The National Targeting Center (NTC) – A single location for targeting technology and subject matter expertise;
- The Automated Targeting System (ATS) – The premier tool employed by CBP personnel to identify high-risk targets in the ocean, as well as other cargo environments;
- The 24-Hour Rule and the Trade Act of 2002 – New regulations that give CBP the authority and mechanisms needed to require advance electronic cargo information prior to arrival or departure from the United States;
- The Container Security Initiative (CSI) – A means of pushing our borders outward by screening cargo overseas and working jointly with host nation customs agencies on exams prior to lading U.S. bound cargo; and
- Non-Intrusive Inspection Technology – Advanced inspection equipment to screen shipments rapidly for WMD, nuclear or radiological materials, terrorist weapons, and other contraband.

(b) Is the supervision of people and cargo in the United States undertaken by separate agencies (immigration and customs) or is it undertaken by one and the same body? If there is more than one agency involved, do these agencies share information and coordinate their activities?

The merger of the U.S. Customs Service, the U.S. Agriculture Plant & Health Inspection Service, the U.S. Immigration and Naturalization Service, and the U.S. Border Patrol in March 2002 created U.S. Customs and Border Protection (CBP) within the newly established Department of Homeland Security. As a result of the merger, for the first time in the history of the United States, all agencies of the United States Government with authorities and responsibilities at our Nation's borders have been unified into a single federal agency. CBP is responsible for managing, controlling and securing the border both at and between the official ports of entry. This includes responsibility for the movement of people and cargo arriving internationally to, and exiting internationally out of, the United States. CBP also works closely with the Transportation and Security Administration (TSA) by supporting and assisting TSA's efforts in the supervision of people and cargo in the continental United States.

(c) How does the United States monitor its borders between ports of entry in order to satisfy itself both that these areas are not being used to undertake terrorist activities against its neighbours and to defend itself against possible infiltration by terrorists? Does the United States have arrangements to cooperate with bordering States in order to prevent cross-border terrorists' acts? If so, please elaborate.

In March 2002, the U.S. Border Patrol became part of U.S. Customs and Border Protection. CBP currently has approximately 11,000 Border Patrol agents whose primary responsibility is to monitor the borders of the United States between the official ports of entry to prevent the entry of terrorists or terrorist weapons into the United States.

The Border Patrol apprehends approximately 1,000,000 people attempting to illegally enter the United States every year. As part of CBP, the Border Patrol has established a link to the National Targeting Center (NTC) in Reston, Virginia, which has immediate access to databases that contain information regarding individuals linked to terrorist activities. The Border Patrol uses the CBP National Targeting Center as a viable resource when a person of interest is encountered while on patrol.

Over the last few years, the Border Patrol has significantly increased its enforcement presence along all our borders by deploying additional personnel, technology, and infrastructure (fences and barriers) along the immediate border area. Headquarters Border Patrol (HQBOR) is currently looking at the possibility of using Unmanned Aerial Vehicles (UAV's) to help in patrolling the border.

The Border Patrol now has over 1,000 agents patrolling the northern border with Canada and an additional 10,000 along the SW Border with Mexico.

Border Patrol has over:

- 8,000 vehicles of all types that we use to patrol the border;
- 100 plus aircraft are used to keep an eye on the sky;
- 118 Certified agents patrol on horseback;
- 294 Bike Patrol Agents are used along the border and in the city;
- 318 K-9 Units are used at the checkpoints and along the border; and
- 480 Agents on ATV's (all terrain vehicles) are also used in rough terrain areas of operation.

Technology:

- Over 14,000 sensors are planted along the border (Seismic, infrared and magnetic);
- 300 RVS Cameras keep an eye on popular border crossings and areas of high interest;
- 260 radio dispatchers work round the clock (24/7) and provide valuable communications services; and
- 120 electronic technicians help maintain the system.

Fencing:

- Border Patrol has over 84 miles of primary and secondary fencing that extends from San Diego, California to Arizona.

- *Does the United States have arrangements to cooperate with bordering States in order to prevent cross-border terrorists' acts? If so, please elaborate.*

In addition to bilateral anti-terrorism initiatives with Mexico on the southern border and Canada on the northern border, Customs and Border Protection works closely with local and state law enforcement authorities using Memoranda of Understanding and/or Memoranda of Agreement for the coordination of enforcement activities including countering terrorism throughout the nation.

(d) As regards international flights, does the United States use advanced passenger manifest programs to check the list of inbound passengers against information, contained in databases on terrorism, before they land?

CBP requires air carriers to transmit passenger and crew manifest data to CPB's Advance Passenger Information System (APIS). The carrier sends this data, electronically, to its data center in Newington, Virginia, where it is processed through our law enforcement databases and run against terrorist indices, prior to the flight's arrival. CBP uses this data as a risk management technique to identify targets and focus its attention on specific passengers and crew, while facilitating the entry of those who pose no risk.

(e) The CTC is encouraged to see that the United States has acceded to Annex 17 of the Convention on International Civil Aviation. Could the United States inform the CTC as to the agency or agencies which are responsible for Airport and Seaport

security? If this agency or these agencies are distinct from the United States' police forces, how is information concerning terrorist threats passed on to these organizations? Are periodic security audits performed at airports and seaports? Is access to port facilities controlled? If so, how? Are airport and seaport personnel screened and provided with identity cards to prevent access by unauthorized personnel to these facilities.

The Transportation Security Administration (TSA) within the Department of Homeland Security (DHS) has statutory responsibility for security of all U.S. airports. The tools it uses include intelligence, regulation, enforcement, inspection and screening, and education of carriers, passengers and shippers. DHS collects, analyzes and disseminates relevant intelligence and threat information. When the information concerns a U.S. airport, this information is passed on to TSA. Periodic inspections are performed at all U.S. airports that have scheduled domestic and/or international flight service and airport identification cards are required for all personnel with access to non-public areas of all U. S. airports that have scheduled domestic and/or international flight service.

- *Are detection devices in place to screen passengers and cargo for weapons and hazardous materials?*

All CBP officers are equipped with personal radiation detectors. In addition, CBP has deployed radiation portal monitors and radiation isotope identifiers as well as technologies for detecting explosive materials. The CBP Canine Enforcement Program is the first Canine Program that has successfully deployed explosive detector dog teams with the ability to search people along with the traditional conveyances and cargo. The CBP Canine Enforcement Program also is the first national canine program to test the feasibility and practicality of deploying canines throughout the nation's borders with the capability of detecting chemical weapons.

- *Are hazardous materials segregated and secured in cargo movements both by air and at sea?*

Unless the hazardous material is selected for inspection, CBP is not responsible for the actual movement and or segregation of hazardous materials in an airport or seaport environment. In the event the material is chosen for inspection, CBP utilizes the ports' Hazardous Materials Specialists to inspect and determine whether a material is safe.

1.9 Sub-paragraph 2 (c) of the Resolution requires States to deny safe heaven to terrorists and their supporters. In this regard, could the United States please provide the CTC with an outline of the legislative provisions regarding the granting of citizenship or other civic rights? Can a foreigner, who is granted citizenship, change his name? What precautions are taken to establish the true identity of a person before new identity papers are issued to that person?

Under the Fourteenth Amendment to the Constitution of the United States, "[a]ll persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside." The statutory provisions governing the granting of United States citizenship, a process known as "naturalization," are found at Title 8, United States Code, sections 1421, et seq. Until recently, the authority to grant citizenship to persons not born in the United States was vested solely in the Attorney General. In 2003, that authority was transferred to the Secretary of Homeland Security, pursuant to the Homeland Security Act. However, the naturalization process remains the same. Among the prerequisites for naturalization, with certain limited exceptions, are that the applicant reside in the United States as a permanent resident for at least five years immediately prior to applying for naturalization, continue that residency throughout the period of application, and establish good moral character (8 U.S.C. sec. 1427). The burden of proof to demonstrate lawful admission to the United States for the purpose of permanent residence is upon the applicant for naturalization (8 U.S.C. sec. 1429). The law requires that applicants furnish photographs (8 U.S.C. sec. 1444) in addition to the biographical information sought in the application, which must be signed in the applicant's own handwriting (8 U.S.C. sec. 1445). Unless waived by the Secretary for Homeland Security, a background investigation of the applicant is conducted by the relevant authorities (8 U.S.C. sec. 1446). An applicant is permitted to petition a court to legally change his or her name, and the new name will be entered on the certificate of naturalization (8 U.S.C. sec. 1447). In general, subsequent name changes are handled in accordance with requirements of state law. Any application for a new certificate of naturalization, based upon a subsequent legal name change, must be accompanied by photographs in accordance with the aforementioned federal statute (8 U.S.C. sec. 1444).

Controls on preventing access to weapons by terrorists

1.10 Sub-paragraph 2 (a) of the Resolution requires each Member State, inter alia, to have in place appropriate mechanisms to deny terrorists access to weapons. In this context, the legislation exposed by the United States in their two reports shows that the violation of arms regulations can be prosecuted and punished. Nevertheless, it doesn't seem that any of these provisions practically deny access to weapons by individuals who may commit terrorist acts:

- *If they are American citizens or legal aliens;*
- *Or, people with no criminal background.*

In these cases, how does the United States intend to meet with the requirement of sub-paragraph 2 (a) of the Resolution?

The Gun Control Act, 18 U.S.C. section 922(g) (GCA), sets forth nine categories of persons who generally cannot legally possess firearms or ammunition in the United States. These categories include felons, persons with misdemeanor crimes of domestic violence (MCDV) convictions, illegal aliens, and non-immigrant aliens. While the CTC is correct that the GCA would not prevent a U.S. citizen or permanent resident alien with no felony or MCDV convictions, or other GCA prohibitions, from possessing firearms, the U.S. has taken numerous steps to prevent terrorists from accessing firearms.

After September 11, 2001, the United States changed its background check system to ensure prohibited illegal and non-immigrant aliens were not able to purchase firearms from federal firearms licensees (FFLs). The form individuals complete before buying a gun from an FFL (ATF Form 4473, Firearms Transaction Record), was amended to ask for any non-U.S. citizen's Bureau of Immigration and Customs Enforcement (ICE) alien or admission number. Any person who is a non-U.S. citizen is now run through the ICE database as part of their National Instant Criminal Background Check System (NICS) check performed by the Federal Bureau of Investigation. Moreover, all non-US citizens, including legal aliens, must show FFL documentation demonstrating they have lived in a state for at least 90 days to be eligible to purchase a firearm. These measures ensure that while permanent resident aliens can legally obtain firearms in the U.S., they are given close scrutiny before such a purchase can occur.

In addition, although a terrorist who did not fall within any of the prohibited categories contained in the GCA would not be prohibited from receiving or possessing firearms or ammunition in the United States, the United States has enacted a procedure for reducing the chances of a terrorist obtaining such weapons. Now, as part of the NICS check, a check is done of the Violent Gang and Terrorist Organization File database. If there is a data match, the firearm purchase is automatically delayed, giving the government a chance to evaluate the purchaser. The purchaser's record is carefully scrutinized to determine whether it is at all possible that he falls within one of the prohibited categories, allowing the purchase to be denied under the GCA.

Furthermore, after September 11, 2001, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) imposed restrictions on non-US citizens temporarily importing firearms into the United States. Effective February 5, 2002, any non-U.S. citizen temporarily importing firearms or ammunition for sporting purposes must obtain an approved ATF Form 6NIA from ATF before importing these items. Such persons previously were able to bring firearms and ammunition into the United States without any permit. Now, before the permit is approved, ATF reviews the specific firearms and ammunition the person intends to bring into the United States and the identity of the person intending to bring them in.

Finally, it should be noted that federal law in the United States generally prohibits all persons from possessing certain firearms that are likely the most appealing to terrorists, including machineguns and semiautomatic assault weapons. 18 U.S.C. sec. 922(o) and (v).

1.11 The first explanations provided by the United States on firearms legislation seem only applicable to the federal level, but it appears that the legislation could be very different at States level and eventually more flexible. So, it is difficult for the CTC to evaluate what is the status of arms in the United States and what are in practice the existing measures to effectively prevent access to weapons by individuals who are intending to commit terrorist acts. The CTC would be grateful to the United States for any explanations or precisions on that purpose.

Federal firearms restrictions apply to all covered individuals and dealers. While states may enact additional laws, they can not be less restrictive. For example, federal law does not restrict the number of firearms an individual may lawfully purchase. However, some states restrict purchases to one firearm per month. In addition, under federal law

not all firearms are treated the same. The sale and possession of particularly dangerous weapons that might be used by terrorists, such as automatic and sawed-off weapons, firearms that have had their serial numbers altered or obliterated, and destructive devices are restricted and subject to more stringent requirements.

1.12 In relation to its legal system on firearms, can the United States give more information on the following items:

- *What are the conditions an individual (US national or legal alien) has to meet under the United States' law to entitle him to purchase firearms?*

First, an individual must not fall into any of the nine prohibited categories under the GCA discussed in the response to question 1.10. A purchase by a felon, or an individual with an MCDV conviction, is prohibited under the GCA. Second, if the individual is purchasing the firearm from an FFL, the individual must execute ATF Form 4473, and successfully undergo a NICS background check by the FBI. As discussed above, this background check involves checks of immigration and terrorist databases. Third, ATF Ruling 2004-1 requires that alien purchasers show that they have resided in a State continuously for at least 90 days immediately prior to the FFL conducting the NICS check. If an alien leaves the United States, the 90-day period stops and restarts from day one when they enter the United States again. The NICS check of the ICE database will show whether a non-immigrant alien has entered or exited the United States in the last 90 days. If there is evidence that a non-immigrant alien has entered or exited the country in the last 90 days, NICS will tell the FFL to cancel the transaction

- *What type(s) of firearms may an individual possess? How many firearms of a particular type may an individual possess? Are there any exceptions in that regard?*

As discussed in the answer to 1.10, certain firearms are banned from civilian possession. Section 922(o) of the GCA provides that it is unlawful for any person to transfer or possess a machine gun not lawfully possessed prior to May 19, 1986. Semiautomatic assault weapons and large capacity ammunition feeding devices are also generally banned under the GCA (See 18 U.S.C. sec. 922(v) and (w).

Certain firearms are regulated under both the GCA and the National Firearms Act, 26 U.S.C. Chapter 53 (NFA). Firearms subject to regulation under the NFA include

machine guns, shotguns having a barrel of less than 18 inches, rifles having a barrel of less than 16 inches, silencers, and destructive devices such as bombs, grenades, rockets and missiles. All NFA weapons must be registered with ATF in the National Firearms Registration and Transfer Record unless they are in the possession or under the control of the United States. See 26 U.S.C. sec. 5841(a). NFA weapons must be registered before they can be lawfully possessed. Under Section 5812(b), NFA weapons cannot be transferred without the approval of the Attorney General. An application must be filed with ATF to transfer an NFA weapon, and a fingerprint based background check is conducted on the transferee prior to transfer. See 26 U.S.C. sec. 5812(a). The purpose of this check is to ensure that NFA weapons are not transferred to persons who cannot lawfully possess them. In addition, taxes are imposed on the transfer and making of NFA weapons under NFA sections 5811 and 5821.

There is no limit under federal law as to how many firearms an individual may possess. However, federal law does require FFLs to report the sales of multiple handguns to one purchaser to ATF by close of business on the day of the transfer on an ATF Form 3310.4, Report of Multiple Sale or Other Disposition of Pistols and Revolvers.

- *What kind of federal measures have been taken by the United States to coordinate the different legislations on firearms adopted in the various States?*

Under the United States Constitution, while the federal government may impose certain restrictions on the possession of certain types of firearms, the individual states may also pass their own laws. Although state law can not authorize what the federal law prohibits, it can be more restrictive. It should be noted that each individual state is represented in both houses of the United States Congress.

ATF provides a publication for the use of FFLs and others listing all relevant state laws entitled ATF Publication 5300.5, State Laws and Published Ordinances.

1.13 Does the United States Custom Service implement Recommendation of WCO Concerning the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organized Crime (29th June 2002)? If yes, please outline the measures applicable in the United States.

In response to how the Department of Homeland Security, ICE implements the "Recommendation of WCO Concerning the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organized Crime." ICE has operational oversight over a broad range of investigative activities related to the enforcement of U.S. export laws, including the illegal export of firearms and ammunition. These laws pertain to the import and export of U.S. defense articles and controlled commodities, and the enforcement of U.S. economic sanctions and embargoes, with an emphasis towards preventing international terrorists and hostile nations from obtaining small arms and light weapon systems, ammunition, and weapons of mass destruction components and related technology from U.S. and foreign sources.

ICE works closely with other U.S. law enforcement agencies, including ATF to facilitate the coordination of joint firearms trafficking investigations; establish policy and procedures through which ICE can exploit, for investigative purposes, the results of firearms traces conducted by ATF; and participate in foreign firearms trafficking conferences to provide international training in firearms trafficking investigative techniques.

1.14 Is it necessary to lodge, register or check the Goods Declaration and supporting documentation concerning firearms prior to their import, export or transit? In addition, is it necessary to encourage importers, exporters or third parties to provide information to the United States' Customs authorities prior to the shipment of such goods?

Imports of handguns, rifles and shotguns require the importer to declare the weapons and to have a permit (ATF-6 form) from ATF. The transit and export of handguns and rifles requires either a Department of State license or license exemption for each shipment, and the Shipper's Export Declaration must be presented to CBP citing the license or license exemption. Customs and Border Protection seeks informed compliance with U.S. laws regarding firearms. Violations of the regulations may result in the seizure of the weapons or further legal action.

With respect to importation of firearms by aliens, on February 5, 2002, ATF published a rule requiring non-immigrant aliens bringing firearms and ammunition into the United States for hunting or sporting purposes to obtain an import permit from ATF.

Prior to the publication of the rule, non-immigrant aliens could do so without a permit. In the interest of national security and public safety, ATF now requires non-immigrant aliens to obtain import permits for all importations of firearms and ammunition into the United States. Non-immigrant aliens who wish to import firearms and ammunition must submit to ATF an ATF Form 6NIA, Application and Permit for Temporary Importation of Firearms and Ammunition by Non-immigrant Aliens. The Form 6NIA requires alien applicants to list identifying information, including their ICE alien or admission number.

1.15 Are there appropriate mechanisms in place to verify the authenticity of licenses and other official documents in relation to the import, export or transit of firearms?

The original ATF-6 form must be presented to CBP at time of import and the exporter must present an original license and file the Shipper's Export Declaration for the export against that license. Additionally, CBP receives a download nightly of all licenses issued by the Department of State.

1.16 Have the United States implemented, using risk assessment principles, appropriate security measures concerning the import, export and transit movement of firearms? In that context, does the United States conduct security checks on the temporary storage, warehousing and transportation of firearms? Does the United States require persons involved in these operations to undergo security vetting?

Persons engaged in the business of importing firearms must first apply and be granted a license as an importer of firearms under the GCA. Any person, including a licensed importer, who wishes to import firearms must also obtain an approved import permit (Form 6) from ATF as discussed above. The Form 6 requires the applicant to list their name and address, as well as that of the broker, the foreign seller and any foreign shipper. The Form 6 requires specific information about the firearms to be imported, including serial number. Importers must also be registered pursuant to the Arms Export Control Act, 22 U.S.C. sec. 2778 (AECA). The export provisions of the AECA are administered by the United States Department of State. To export firearms, persons must first obtain a valid export license from the State Department under the AECA.

Import shipments of firearms and other goods may be stored in Customs Bonded Warehouses (CBWs) and Foreign Trade Zones (FTZs). Customs regulates the functioning of CBWs and FTZs. Under its inspection authority granted by the provisions of the GCA, ATF has the authority to inspect firearms shipments being stored in CBWs.

Customs conducts security checks on carriers, and warehousing facilities for all commodities to ensure compliance with CBP regulations. Additionally, Customs requires carriers and warehouse operations to carry bonds to cover any penalties or other sanctions. Background checks are conducted on person involved in these operations.